REMARKS

Claims 10, 17, and 22 were previously cancelled. Claims 1-9, 11-16, 18-21, and 23-26 remain in the Application. Reconsideration of the pending claims is respectfully requested in view of the following remarks.

I. Claims Rejected Under 35 U.S.C. § 103(a)

Claims 1-9, 11-16, 18-21, and 23-26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pre-Grant Publication No. 2002/0015494 applied for by Nagai, et al. ("Nagai"). Applicants respectfully traverse the rejection.

To establish a *prima facie* case of obviousness, the Examiner must show the cited references, combined, teach or suggest each of the elements of a claim. Claim 1 recites:

> "a number generator housed in a host device to generate a nonce; and an encryption subsystem housed in a storage device to encrypt data .... using an encryption bus key prior to transmitting the encrypted data via a data bus to the host device in which the encrypted data is to be decrypted, and said encryption bus key is derived based on.... the nonce received over the data bus from the number generator." (Emphasis added).

Applicants submit that Nagai does not teach or suggest each of the elements of the claim.

Nagai discloses a system in which an illegally produced data storage medium (e.g., a DVD) is prevented from being played. On a legally produced DVD, stored data is scrambled and superimposed with a watermark (FIG. 1). Before playing the DVD, a compliant player descrambles the stored data and decodes the watermark to detect whether the DVD is legally produced (FIG. 10). Nagai discloses that a scrambler is implemented in a PC encoder connecting to a recording drive (FIG. 7), and a descrambler is implemented in a PC decoder connecting to a playback drive (FIG. 10). In FIG. 2B, a random number generator is used in the scrambling process to generate a title key.

The Examiner characterizes the random number generator of FIG. 2B as the claimed number generator housed in a host device, and also characterizes the encryption unit 914 in the playback drive of FIG. 10 as the claimed encryption subsystem housed in a storage device. However, encryption unit 914 does not encrypt data using a nonce generated by the random number generator as required by the encryption subsystem of Claim 1. Rather, the nonce generated by the random number generator is used by a scrambler 610 in the PC encoder (FIG.

7). There is nothing in Nagai disclosing that encryption unit 914 uses the random number generator of FIG. 2B. Thus, encryption unit 914 cannot be the claimed encryption subsystem. Further, Nagai discloses that the random number is used as a title key in the scrambler located in the PC encoder of FIG. 7. The PC encoder (a host device) uses the title key (a random number) to encrypt and scramble video data, and records the data onto the DVD (FIG. 2B). Thus, it is encryption unit 614 in a host device, rather than encryption unit 914 in a storage device, that encrypts data using a random number. However, encryption unit 614 also cannot be the claimed encryption subsystem, because encryption unit 614 is housed in a host device instead of the claimed storage device. As Claim 1 requires that the encryption subsystem be housed in a storage device to encrypt data....using the nonce, neither encryption unit 614 nor 914 teaches or suggests the claimed encryption subsystem.

Nagai's system uses the random number for a purpose different from the claimed system. Nagai's system is designed to prevent the playback of illegally reproduced data medium (e.g., a DVD). The claimed system on the other hand prevents data to be illegally reproduced by a replay attack. A replay attack happens when encrypted data is transmitted from the storage device to the host device over a data bus (the specification at paragraph 16). The claimed system prevents the replay attack by ensuring that the nonce transmitted during replay is different from the nonce used to generate the bus key (paragraph 16 of the specification at page 6, lines 11-14). Thus, an attacker would not be able to obtain the nonce on which the bus key is based by intercepting the data bus during replay. By contrast, Nagai discloses that the random number of FIG. 2B is encrypted and stored on the same disk as the scrambled data. Thus, the encrypted random number can be read at the same time when the encrypted data is read. Thus, the random number disclosed by Nagai for data scrambling cannot be effectively used for preventing a replay attack.

The Examiner recognizes that Nagai does not disclose how the bus key is generated, but indicates that it would have been obvious to generate the claimed bus key in a manner similar to the title key disclosed by Nagai. Contrary to the Examiner's assertion, Nagai indeed discloses how the bus key is generated. In paragraphs 165-171 and FIG. 14, Nagai describes that a time-variant key is generated for transferring data over the data bus between a DVD drive and a MPEG decoder (e.g., decoder 408 or decoder 908 in a host device). The time-variant key protects data transmitted over the data bus and may be viewed as a bus key. Nagai specifically

discloses that the time-varying key is based on a random number generated by the DVD drive (paragraph 168). The claimed system requires that the random number be generated by a host device. Thus, Nagai has effectively taught away the claimed bus key that is generated by the host device.

Analogous discussion applies to amended Claims 11 and 18. In regard to Claims 2-9, 12-16, 19-21, and 23-26, these claims depend from independent Claims 1, 11, and 18 and incorporate the limitations thereof. Thus, for at least the reasons mentioned in regard to Claims 1, 11, and 18, these dependent claims are not obvious over Nagai.

Moreover, with respect to Claims 3-4, 14, and 19, the Examiner relies on the function disclosed in paragraphs 167-168 for disclosing the claimed one-way function. However, there is nothing in Nagai that mentions the disclosed function generates the encryption bus key based on a media key and the nonce. The function disclosed by Nagai instead receives only a random number from the DVD drive as input. Assuming for the sake of argument Nagai's function is a one-way functions, the input to the function is different from the claimed media key and the nonce. Thus, Claims 3-4, 14, and 19 is not obvious over Nagai for this additional reason.

Accordingly, reconsideration and withdrawal of the obviousness rejection of Claims 1-9, 11-16, 18-21, and 23-26 are requested.

CONCLUSION

In view of the foregoing, it is believed that all claims now are now in condition for allowance and such action is earnestly solicited at the earliest possible date. If there are any additional fees due in connection with the filing of this response, please charge those fees to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: June 29, 2006

Thomas Coester

Thomas M. Coester, Reg. No. 39,367

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
Telephone (310) 207-3800
Facsimile (310) 820-5988

CERTIFICATE OF FACSIMILE

I hereby certify that this correspondence is being transmitted via facsimile on the date shown below to the United States Patent and Trademark Office.

Amber D. Saunders 6/29/06

Amber D. Saunders Date